

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEIZURE OF:) Case No.: 1:23-SW-216

**Five Domain Names Registered at Public
Interest Registry (PIR)**)

IN THE MATTER OF THE SEIZURE OF:) Case No.: 1:23-SW-217

**Eight Domain Names Registered at
Verisign, Inc.**)

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, Tina Show-Hwa Chang, being first duly sworn, hereby depose and state as follows:

INTRODUCTION

1. I am a Special Agent with the Department of Commerce (“DOC”), Bureau of Industry and Security (“BIS”), Office of Export Enforcement (“OEE”), and I have been so employed since August 2015. I am empowered by law to investigate and make arrests for offenses involving the unlawful export of goods, technology, and services to destinations outside the United States. As a special agent for OEE, I am responsible for investigating violations of laws relating to the export of controlled commodities and technology from the United States. As part of my training as a special agent, I have completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center as well as other federal training programs, to include courses on how to conduct cyber investigations.

2. During the course of my duties as a special agent, I have conducted and supported numerous investigations involving the illegal export of items from the United States and illicit

procurement by terrorist organizations. As part of these investigations, I have participated in interviews of suspects and witnesses, conducted surveillance, and assisted with the execution of court-authorized search warrants. I have also obtained and analyzed data and evidence from a variety of sources, including electronic communications, and used other investigative techniques to secure relevant information and evidence regarding various criminal activities. As a result of my training and experience, I am familiar with techniques and methods of operation used by individuals and illicit procurement networks that are involved in the illegal export of items from the United States and illicit procurement by terrorist organizations, as well as technique and methods used to evade detection by U.S. law enforcement.

3. I am an “investigative or law enforcement officer of the United States” within the meaning of 18 U.S.C. § 2510(7). As such, I am empowered to conduct investigations of and to make arrests for offenses enumerated in 50 U.S.C. § 1705 (International Emergency Economic Powers Act).

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

5. As set forth below, there is probable cause to believe that the following 13 domain names – moqawama.org, almanarnews.org, manarnews.org, almanar-tv.org, and alshahid.org (which utilize Public Interest Registry (“PIR”) as their domain registry), as well as manartv.net, manarnews.net, almanar-tv.com, almanar-tv.net, alidaamouch.com, Ibrahim-alsayed.net, alemdad.net, and naimkassem.net (which utilize VeriSign as their domain registry) (hereinafter,

“SUBJECT DOMAIN NAMES”) – constitute violations of 50 U.S.C. § 1705 (IEEPA) and 31 C.F.R. § 594.201.

6. As further described in this affidavit, Specially Designated Nationals¹ (“SDNs”), Specially Designated Global Terrorists² (“SDGTs”), and their members utilize the VeriSign, Inc. and PIR domain registries for their websites. This utilization, regardless of content, is a violation of 50 U.S.C. § 1705 and 31 C.F.R. § 594.201 (the “SUBJECT OFFENSES”), which prohibit SDNs and SDGTs, such as Lebanese Hizballah, Al Manar TV, Ali Damush, Ibrahim al-Sayyid, Islamic Charitable Emdad Committee, Martyrs’ Foundation in Lebanon, Naim Qasim, and their members from obtaining services, including website and domain services, in the United States without a license from the Office of Foreign Assets Control (“OFAC”). As set forth below, these entities do not have a license to utilize the SUBJECT DOMAIN NAMES. Additionally, the SUBJECT DOMAIN NAMES are assets of an SDN or SDGT engaged in planning or perpetrating a federal crime of terrorism or that afford any person a source of influence over such an entity or organization. They are therefore subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i), and the utilization of the SUBJECT DOMAIN NAMES is in violation of the SUBJECT OFFENSES.

7. I make this affidavit for a warrant to seize the property described in Attachment A, incorporated herein by this reference, specifically, the SUBJECT DOMAIN NAMES. The

¹ Specially Designated Nationals are entities designated pursuant to the programs listed in Chapter V, Title 31 of the Code of Federal Regulations. A complete list of Specially Designated Nationals is available on the Department of the Treasury’s website.

² Title 31, Code of Federal Regulations, Section 594.310 defines a Specially Designated Global Terrorist as any person whose property and interests are blocked pursuant to 31 C.F.R. § 594.201(a).

procedure by which the United States will seize the SUBJECT DOMAIN NAMES is described in Attachment A hereto and below.

BACKGROUND ON DOMAIN NAMES

8. Based on my training and experience and information learned from others, I am aware of the following:

9. Internet Protocol Address: An Internet Protocol address (“IP address”) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g. 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. An IP address acts much like a home or business street address – it enables computers connected to the Internet to properly route traffic to each other. The assignment of IP addresses to computers connected to the Internet is controlled by Internet Service Providers (ISPs).

10. Domain Name: A domain name is a simple, easy-to-remember way for humans to identify computers on the Internet, using a series of characters (e.g. letters, numbers, or other characters) that correspond with a particular IP address. For example, “usdoj.gov” and “cnn.com” are domain names.

11. Domain Name System: The domain name system (“DNS”) is, among other things, a hierarchical convention for domain names. Domain names are composed of one or more parts, or “labels,” that are delimited by periods, such as “www.example.com.” The hierarchy of domains descends from right to left; each label to the left specifies a subdivision, or subdomain, of the domain on the right. The right-most label conveys the “top-level” domain. For example, the

domain name “www.example.com” means that the computer assigned that name is in the “.com” top-level domain, the “example” second-level domain, and “www.” is the web server.

12. Domain Name Servers: DNS servers are computers connected to the Internet that convert, or resolve, domain names into IP addresses.

13. Registry: For each top-level domain (such as “.com”), there is a single company, called a “registry,” that determines which second-level domain resolves to which IP address. For example, the registry for the “.com” and “.org” top-level domains are, respectively, VeriSign, Inc. (VeriSign), which has its headquarters at 12061 Bluemont Way, Reston, Virginia, and the Public Interest Registry (PIR), which has its headquarters at 11911 Freedom Drive, Reston, Virginia, both within the Eastern District of Virginia.

14. Registrar & Registrant: Domain names may be purchased through a registrar, which acts as the intermediary between the registry and the purchasers of the domain name. The individual or business that purchases, or registers, a domain name is called a “registrant.” Registrants control the IP address, and thus the computer, to which their domain name resolves. Thus, a registrant may easily move a domain name to another computer anywhere in the world. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

15. Whois: A “Whois” search provides publicly available information as to which entity is responsible for a particular IP address or domain name. A Whois record for a particular IP address or domain name will list a range of IP addresses that the IP address falls within and the entity responsible for that IP address range and domain name. For example, a Whois record for the domain name XYZ.COM might list an IP address range of 12.145.67.0 – 12.145.67.99 and

list Company ABC as the responsible entity. In this example, Company ABC would be responsible for the domain name XYZ.COM and IP addresses 12.145.67.0 – 12.145.67.99.

RELEVANT CRIMINAL STATUTES

16. The International Emergency Economic Powers Act (“IEEPA”), 50 U.S.C. §§ 1701-1706, authorizes the President to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States when the President declares a national emergency with respect to that threat.

17. Pursuant to the authority under IEEPA, the President of the United States and the Executive Branch have issued orders and regulations governing and prohibiting certain transactions by U.S. persons or involving U.S. goods. Title 50, United States Code, Section 1705(a), provides that “[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter.” Section 1705(c) provides that a person who willfully commits, willfully attempts to commit, or willfully conspires to commit, or aids or abets in the commission of, an unlawful act described in subsection (a) shall, upon conviction, be fined not more than \$1,000,000, or if a natural person, may be imprisoned for not more than twenty years, or both.

18. On September 23, 2001, the President of the United States issued Executive Order (“E.O.”) 13224 titled “Blocking Property and Prohibiting Transactions with Persons who Commit, Threaten to Commit, or Support Terrorism.” The E.O. is a tool the U.S. Government utilizes to combat the threat of terrorism and to impede support to terrorism. Executive Order 13224 authorizes the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, to designate individuals or entities that he determines have committed, or pose a significant risk of committing, acts of terrorism against U.S. interests. These individuals

and entities may also be designated for providing financial, material, or technological support for, or goods or services to or in support of, for example, Hizballah.

19. The U.S. Department of the Treasury, Office of Foreign Assets Control publishes this list of designated individuals, groups, and entities, such as terrorist organizations and its members. Collectively, such individuals and companies are called “Specially Designated Nationals,” “SDNs,” or “Specially Designated Global Terrorists,” “SDGTs.” Their property and interests are blocked pursuant to 31 C.F.R. § 594.201(a) and the entities are published in the Federal Register and incorporated into OFAC’s SDN List.

20. Section 1 of the Executive Order states, in relevant part, that all property and interests in property of certain persons that are in, or come within the United States, or that come within the possession or control of United States persons are blocked.

21. Section 2(a) of the Executive Order states: “any transaction or dealing by United States persons or within the United States in property or interests in property blocked pursuant to this order is prohibited, including but not limited to the making or receiving of any contribution of funds, goods, or services to or for the benefit of those persons listed in the Annex to this order or determined to be subject to this order[.]”

22. To implement E.O. 13224, the United States Department of the Treasury, through the Office of Foreign Assets Control (“OFAC”), issued 31 C.F.R. § 594 – Global Terrorism Sanctions Regulations (“GTSR”). Without prior authorization from OFAC, this provision prohibits all tangible and intangible transactions with SDNs and SDGTs.³ Additionally, 31

³ Section 594.309 states: “The terms *property* and *property interest* include, but are not limited to, money, checks, drafts, bullion, bank deposits, savings accounts, debts, indebtedness, obligations, notes, guarantees, debentures, stocks, bonds, coupons, any other financial instruments, bankers acceptances, mortgages, pledges, liens or other rights in the nature of security, warehouse receipts, bills of lading, trust receipts, bills of sale, any other evidences of

C.F.R. § 594.406 not only prohibits transactions or dealings involving blocked property with SDNs and SDGTs, but also prohibits services performed in the United States or by U.S. persons, to include technological services provided by U.S. registries such as Verisign and PIR.

23. SDNs and SDGTs violate the SUBJECT OFFENSES by obtaining or utilizing goods or services in the United States without a license from OFAC. Accordingly, the SUBJECT OFFENSES preclude Lebanese Hizballah, Al Manar TV, Ali Damush, Ibrahim al-Sayyid, Islamic Charitable Emdad Committee, Martyrs' Foundation in Lebanon, Naim Qasim, and their members from utilizing or receiving services for the SUBJECT DOMAIN NAMES, which are owned and operated by Verisign Inc. or the Public Interest Registry, U.S. companies based in Reston, Virginia.

Designated Individuals and Entities

24. The individuals and entities below have been designated as a part of E.O. 13224 for having committed acts of terrorism, posing a significant risk for committing acts of terrorism, or for providing financial, material, or technological support to Hizballah.

- a. On October 31, 2001, the U.S. Department of the Treasury designated Hizballah a Specially Designated Global Terrorist (SDGT).
- b. On March 23, 2006, Al Manar TV, a satellite television operation owned or controlled by the Iran-funded Hizballah terrorist network, was designated by the

title, ownership or indebtedness, letters of credit and any documents relating to any rights or obligations thereunder, powers of attorney, goods, wares, merchandise, chattels, stocks on hand, ships, goods on ships, real estate mortgages, deeds of trust, vendors' sales agreements, land contracts, leaseholds, ground rents, real estate and any other interest therein, options, negotiable instruments, trade acceptances, royalties, book accounts, accounts payable, judgments, patents, trademarks or copyrights, insurance policies, safe deposit boxes and their contents, annuities, pooling agreements, *services of any nature whatsoever*, contracts of any nature whatsoever, and *any other property*, real, personal, or mixed, tangible or *intangible*, or interest or interests therein, present, future or contingent.” (emphasis added)

Secretary of Treasury through OFAC as a Specially Designated National under E.O. 13224 for being the media arm of the Hizballah terrorist network and for facilitating Hizballah's activities. Al Manar TV has supported fundraising and recruitment efforts by Hizballah. The organization raises funds for Hizballah through advertisements broadcast on the network and an accompanying website that requests donations for the terrorist organization.

- c. On January 9, 2017, Ali Damush was designated a Specially Designated Global Terrorist (SDGT) under E.O. 13224. Damush is a senior leader of Hizballah, a Foreign Terrorist Organization (FTO) and SDN, and an aide to its leader, Hassan Nasrallah, a Specially Designated Global Terrorist (SDGT). Damush leads Hizballah's Foreign Relations Department, which engages in covert terrorist operations around the world on behalf of Hizballah, including recruiting terrorist operatives and gathering intelligence.
- d. On May 16, 2018, OFAC designated Ibrahim Al-Amin Al-Sayyid an SDGT for acting for or on behalf of Hizballah. Al-Sayyid is the head of Hizballah's Political Council. He was Hizballah's first official spokesperson and was involved in the formation of Hizballah.
- e. On May 16, 2018, OFAC designated Naim Qasim an SDGT for acting for or on behalf of Hizballah. Qaim is the Deputy Secretary General of Hizballah and joined the organization in the early 1980s. Before ascending to his current position, he served as the Deputy President of the Executive Council.
- f. On August 3, 2010, OFAC designated the Islamic Charitable Emdad Committee, also known as the Imam Khomeini Relief Committee (IKRC) Lebanon Branch, a

Specially Designated National. The IKRC in Lebanon is a Hizballah social service organization that was created by the Government of Iran in the 1980s and is directed and run by Hizballah members. Iran has provided millions of dollars to the Hizballah-run branch in Lebanon since 2007. The IKRC has helped fund and operate Hizballah youth training camps, which have been used to recruit future Hizballah members and operatives. Hizballah Secretary General Hassan Nasrallah has acknowledged the IKRC branch in Lebanon as one of Hizballah's openly-functioning institutions linked to and funded by Iran.

- g. In July 2007, OFAC designated the Martyrs Foundation in Lebanon an SDN. The Martyrs Foundation is an Iranian parastatal organization that channels financial support from Iran to several terrorist organizations in the Levant, including Hizballah and the Palestinian Islamic Jihad (PIJ). Martyrs Foundation branches in Lebanon have also provided financial support to the families of killed or imprisoned Hizballah and PIJ members, including suicide bombers in the Palestinian territories.

25. Hizballah, Al Manar TV, Ali Damush, Ibrahim Al-Amin Al-Sayyid, Naim Qasim, the Islamic Charitable Emdad Committee, and the Martyrs Foundation in Lebanon will hereafter be referred to collectively as the SUBJECT ENTITIES and have engaged in terrorism against the U.S. as described in 18 U.S.C. § 981(a)(1)(G)(i).

26. SDNs and SDGTs violate the SUBJECT OFFENSES by obtaining or utilizing goods or services in the United States without a license from the Office of Foreign Assets Control. Accordingly, the SUBJECT OFFENSES preclude SUBJECT ENTITIES or their members from utilizing the SUBJECT DOMAIN NAMES, which are owned and operated by Verisign Inc. and

PIR, United States companies based in Reston, Virginia.⁴ The SUBJECT DOMAIN NAMES are thus subject to seizure and forfeiture as noted in paragraph 6 above.

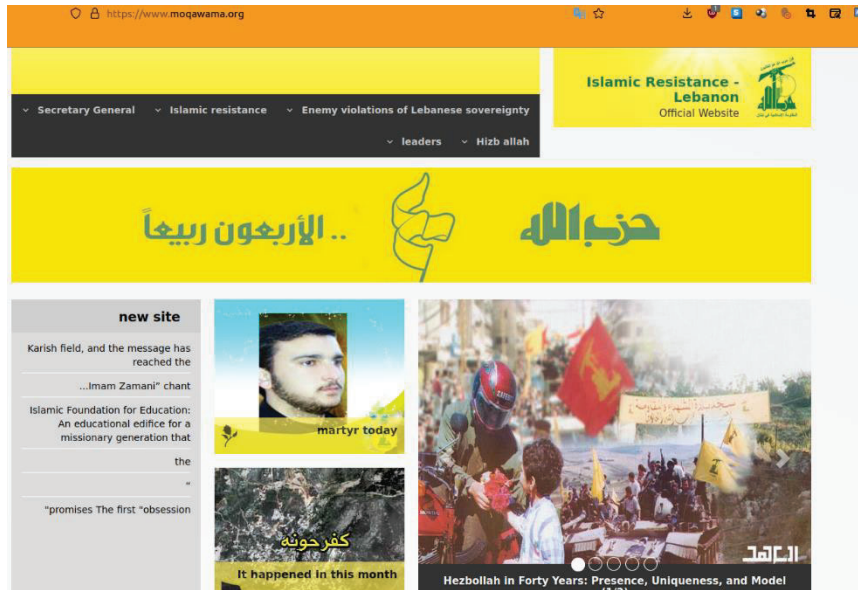
**CASE BACKGROUND AND PROBABLE CAUSE FOR DOMAINS UTILIZED FOR
OFAC DESIGNATED ENTITIES**

27. SDN and SDGT entities have been designated for planning to perpetrate terrorism against the United States or for financially or materially supporting Hizballah, which likewise has and is planning to perpetrate terrorism against the United States. The use of these domains, without prior authorization from OFAC, is prohibited as they are controlled by these entities and utilize a United States-based service. The following domains are used to support SDN and SDGT entities and the content of the domains in this affidavit is used to show that the domains are ultimately the property of and controlled by an SDN or an SDGT. Further, the content of the domains demonstrates that the domains afford a source of influence on behalf of these SDN and SDGT entities.

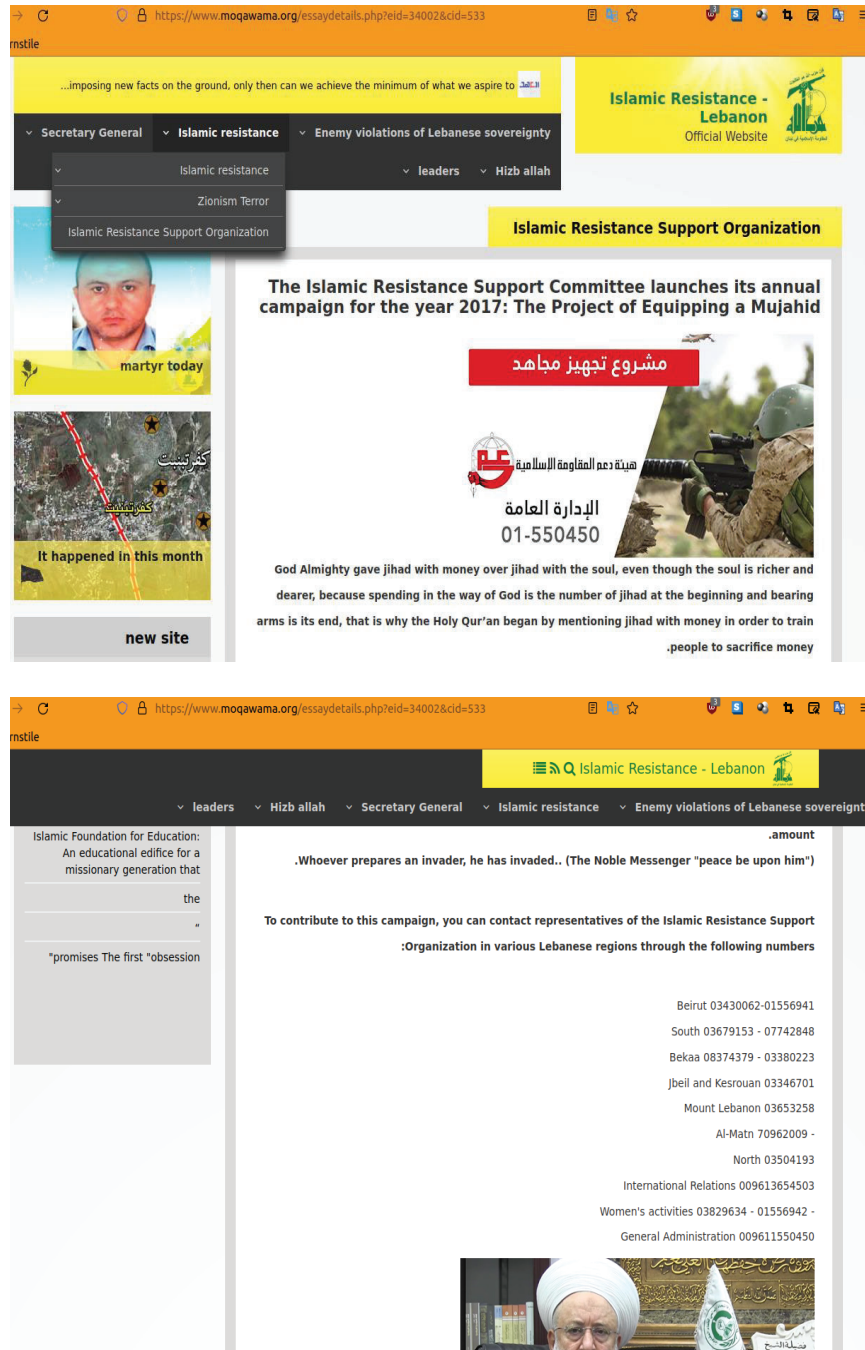
28. Lebanese Hizballah, until September 11, 2001, was responsible for more American deaths than any other terrorist organization. Hizballah is known or suspected to have been involved in numerous terrorist attacks throughout the world, including the suicide truck bombings of the U.S. Embassy and U.S. Marine Corps barracks in Beirut in 1983 and the U.S. Embassy annex in Beirut in September 1984. Hizballah also executed the 1985 hijacking of TWA Flight 847 *en route* from Athens to Rome. In July 2006 Hizballah precipitated a violent conflict that resulted in scores of civilian casualties in Israel and Lebanon. Hizballah was designated as a SDGT under Executive Order 13224 on October 31, 2001.

⁴ This prohibition on the utilization of the SUBJECT DOMAIN NAMES is not based on the content posted to the SUBJECT DOMAIN NAMES. Rather, the violation stems from the mere utilization of the United States-based services without a license from the Office of Foreign Asset Control, as explained further below.

- a. Hizballah's main domain is "moqawama.org."
- b. A screen capture of the domain shows the Hizballah flag in the right corner as well as the words "Islamic Resistance – Lebanon, Official Website":



- c. When navigating the site, there is a tab named "Islamic resistance" with a drop-down menu that shows three options, one of which is "Islamic Resistance Support Organization" (IRSO). When this tab is selected, the entire page is dedicated to IRSO and lists various contacts to call in order to financially support IRSO and ultimately Lebanese Hizballah. Hizballah uses IRSO to solicit donations in support of its terrorist activities and was subsequently designated by the U.S. Department of the Treasury as an SDN on August 29, 2006, Solicitation materials distributed by IRSO inform prospective donors that funds will be used to purchase sophisticated weapons and conduct operations. Donors can choose from a series of projects to contribute to, including supporting and equipping fighters and purchasing rockets and ammunition. IRSO has identified itself to prospective donors as one and the same as Hizballah.



- a. On or about January 12, 2023, I conducted an open-source domain search, reviewed IP and Whois record information, and confirmed that “moqawama.org” was an active domain.

29. Al Manar TV is the media arm of the Hizballah terrorist network. According to the Department of Treasury's designation,⁵ Al Manar TV has raised funds for Hizballah through advertisements broadcast on its network and its website where it requested donations. In addition to helping to finance the organization, Hizballah's Secretary General Nasrallah publicized invitations to Lebanese Citizens to volunteer for Hizballah military training. In one instance, a Hizballah operative, under the cover of employment by Al Manar TV, conducted pre-operation surveillance for the terrorist organization. On March 23, 2006, Al Manar TV, including domains "almanar.com.lb" and "manartv.com" were designated by the Secretary of the Treasury through OFAC as an SDN pursuant to E.O. 13224 because Al Manar TV is owned or controlled by Hizballah.

a. On or about January 12, 2023, I reviewed "almanarnews.org," "manarnews.org," and "manarnews.net." While navigating to these domains, the user is redirected to "almanar.com.lb."

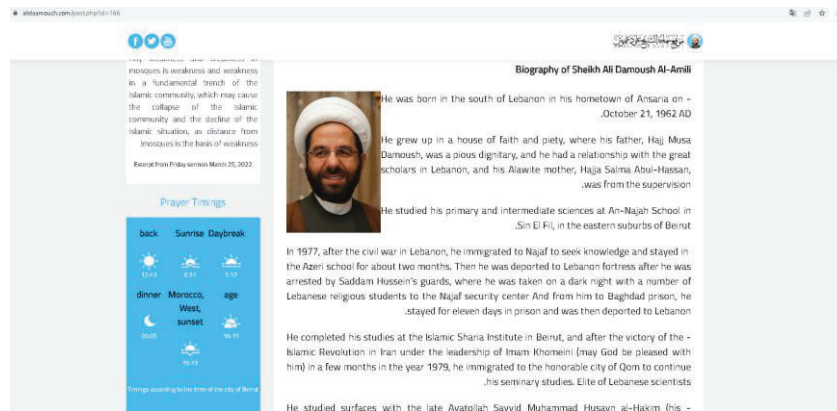
b. On or about January 12, 2023, I reviewed "manartv.net," "almanar-tv.com," "almanar-tv.net," and "almanar-tv.org." These domains appear to be the same webpage as "almanar.com.lb."

c. On or about January 12, 2023, I conducted an open-source domain search, reviewed IP and Whois record information, and confirmed that "almanarnews.org," "manarnews.org," "manarnews.net," "manartv.net," "almanar-tv.com," "almanar-tv.net," and "almanar-tv.org" are active domains.

⁵ See <https://home.treasury.gov/news/press-releases/js4134>.

30. Ali Damush is a senior leader in Hizballah and an aide to the organization's leader, Hassan Nasrallah, a Specially Designated Global Terrorist. Damush leads Hizballah's Foreign Relations Department which engages in covert terrorist operations, recruits terrorist operatives, and gathers intelligence. On January 9, 2017, OFAC designated Ali Damush as an SDGT.

a. Ali Damush appears to utilize the "alidaamouch.com" domain, which has an entire biography tab about himself.



On or about January 12, 2023, I conducted an open-source domain search, reviewed IP and Whois record information, and confirmed that "alidaamouch.com" is an active domain. Additionally, according to information provided by Whois, "alidaamouch.com" is registered to Beirut, Lebanon and provides a particular IP address. The IP address is the same as the one used by "ibrahim-alsayed.net" and "naimkasssem.net" (described below).

31. Ibrahim Al-Amin Al-Sayyid is the head of Hizballah's Political Council. He was Hizballah's first official spokesperson and was involved in the formation of Hizballah. On May 16, 2018, OFAC designated Ibrahim al-Amin al-Sayyid an SDGT.

a. Al-Sayyid utilizes the domain "ibrahim-alsayed.net," which is titled "Mr. Ibrahim Amin El-Sayed's website | Head of the Political Council of Hezbollah."

b. A screenshot of the domain reflects the title in a gray text box at the bottom of the domain as well as a photo of Al-Sayyid speaking at a public event with the Hizballah flag posted in the bottom left corner.

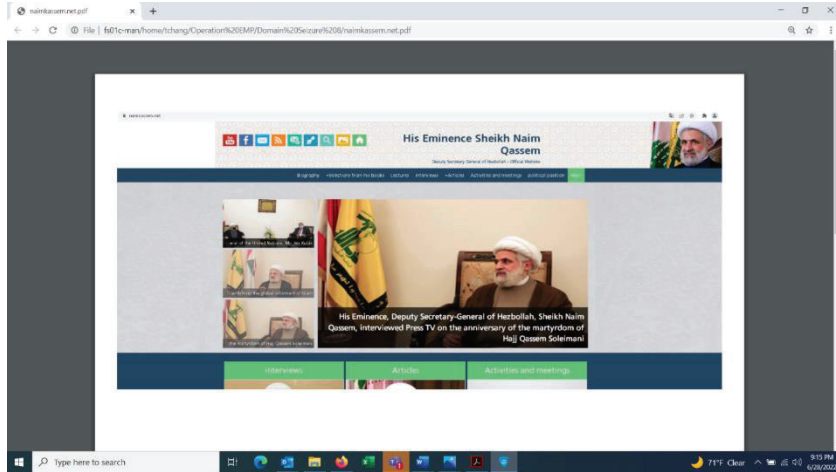


c. On or about January 12, 2023, I conducted an open-source domain search, reviewed IP and Whois record information, and confirmed that “ibrahim-alsayed.net” is an active domain. Additionally, according to information provided by Whois, “ibrahim-alsayed.net” is registered to Beirut, Lebanon and provides a particular IP address. The IP address is the same as the one used by “alidaamouch.com” (described above) as well as “naimkassem.net” (described below).

32. Naim Qasim is the Deputy Secretary General of Hezbollah. On May 16, 2018, OFAC designated Qasim as a Specially Designated National. Qasim utilizes the domain “naimkassem.net,” which reads, “His Eminence Sheikh Naim Qassem, Deputy Secretary General of Hezbollah-Official Website.”

a. A screenshot of the site taken on or about May 11, 2022, shows an article titled “His Eminence, Deputy Secretary General of Hezbollah, Sheikh Naim Qasim, interviewed Press TV on the anniversary of the martyrdom of Hajj Qassem Soleimani.” Qasim is pictured

above the title of the article speaking in front of a Hizballah flag.



b. On or about January 12, 2023, I conducted an open-source domain search, reviewed IP and Whois record information, and confirmed that “naimkassem.net” is an active domain. Additionally, according to information provided by Whois, “naimkassem.net” is registered to Beirut, Lebanon and provides a particular IP address. The IP address is the same as the one used by “alidaamouch.com” and “ibrahim-alsayed.net” (described above).

33. The Islamic Charitable Emdad Committee, also known as the Imam Khomeini Relief Committee (IKRC) Lebanon Branch, is a Hizballah social service organization that was created by the Government of Iran and is directed and run by Hizballah members or cadre. Iran has provided millions of dollars to the Hizballah-run branch in Lebanon since 2007. The IKRC has helped fund and operate Hizballah youth training camps, which have been used to recruit future Hizballah members and operatives. Hizballah Secretary General Hassan Nasrallah has acknowledged the IKRC branch in Lebanon as one of Hizballah’s openly-functioning institutions linked to and funded by Iran. On August 3, 2010, OFAC designated the IKRC as a Specially Designated National. IKRC utilizes the domain “alemdad.org.lb”

a. When navigating to the domain “alemdad.net,” the user is redirected to the domain “alemdad.org.lb.”

b. On or about January 12, 2023, I conducted an open-source domain search, received IP and Whois record information, and confirmed that “alemdad.net” was active.

34. The Martyrs Foundation is an Iranian parastatal organization that channels financial support from Iran to several terrorist organizations, including Hizballah. On or about July 24, 2007, OFAC designated the Martyrs Foundation in Lebanon an SDN. The Martyrs Foundation in Lebanon utilizes the domain “shaheed.com.lb.”

a. When navigating to the domain “alshahid.org” the user is redirected to the domain, “shaheed.com.lb.”

b. On or about January 12, 2023, I conducted an open-source domain search, received IP and Whois record information, and confirmed that “alshahid.org” was active.

35. On or about May 25, 2022, the U.S. Department of the Treasury’s Office of Foreign Assets Control confirmed that the following SDN and SDGT entities – Al Manar TV, Ali Damush, Ibrahim al-Sayyid, Naim Qasim, Islamic Charitable Emdad Committee, and the Martyrs Foundation – did not receive authorization from the agency to utilize services provided by VeriSign or PIR for the following domains: moqawama.org, almanarnews.org, manarnews.org, manartv.net, manarnews.net, almanar-tv.com, almanar-tv.net, almanar-tv.org, alidaamouch.com, Ibrahim-alsayed.net, naimkassem.net, alemdad.net, and alshahid.org. On or about July 21, 2022, the U.S. Department of the Treasury’s OFAC confirmed that SDGT designated Lebanese Hizballah and SDN designated Islamic Resistance Support Organization did not receive authorization from the agency to utilize services provided by PIR for use of the domain moqawama.org.

36. For the reasons discussed above, there is probable cause to believe that violations of the SUBJECT OFFENSES have been committed and that the SUBJECT DOMAIN NAMES

represent violations of 50 U.S.C. § 1705 and 31 C.F.R. § 594.201 and assets of an individual, entity, or organization engaged in planning or perpetrating a federal crime of terrorism or that afford any person a source of influence over such an entity or organization. They are therefore subject to seizure and forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(G)(i).

THE SUBJECT DOMAIN NAMES

37. As described above, the SUBJECT DOMAIN NAMES were used by the SUBJECT ENTITIES to provide services to Hizballah, a Lebanon-based terrorist group as well as a designated SDN and FTO. This utilization, regardless of content, is a violation of 50 U.S.C. § 1705 and 31 C.F.R. § 594.201, which prohibit Specially Designated Nationals and Specially Designated Global Terrorists such as Lebanese Hizballah, Al Manar TV, Ali Damush, Ibrahim al-Sayyid, Islamic Charitable Emdad Committee, Martyrs' Foundation in Lebanon, Naim Qasim, and their members from obtaining services, including website and domain services, in the United States without a license from the Office of Foreign Assets Control.

38. The top-level domain for “moqawama.org,” “almanarnews.org,” “manarnews.org,” “almanar-tv.org,” and “alshahid.org” is PIR. PIR currently manages all “.org” domains.

a. A search of publicly available Whois domain name registration records revealed that “moqawama.org” was registered on or about January 31, 1997.

b. A search of publicly available Whois domain name registration records revealed that “almanarnews.org” was registered on or about October 5, 2010.

c. A search of publicly available Whois domain name registration records revealed that “manarnews.org” was registered on or about October 5, 2010.

d. A search of publicly available Whois domain name registration records revealed that “almanar-tv.org” was registered on or about August 26, 2015.

e. A search of publicly available Whois domain name registration records revealed that “alshahid.org” was registered on or about September 3, 2004.

39. The top-level domain for “manarnews.net,” “manartv.net,” “almanar-tv.com,” “almanar-tv.net,” “alidaamouch.com,” “ibrahim-alsayed.net,” “naimkassem.net,” and “alemdad.net” is Verisign, Inc. Verisign currently manages all “.com” and “.net” domains.

a. A search of publicly available Whois domain name registration records revealed that “manarnews.net” was registered on or about October 5, 2010.

b. A search of publicly available Whois domain name registration records revealed that “manartv.net” was registered on or about August 26, 2015.

c. A search of publicly available Whois domain name registration records revealed that “almanar-tv.com” was registered on or about March 3, 2011.

d. A search of publicly available Whois domain name registration records revealed that “almanar-tv.net” was registered on or about March 3, 2011.

e. A search of publicly available Whois domain name registration records revealed that “alidaamouch.com” was registered on or about July 11, 2019.

f. A search of publicly available Whois domain name registration records revealed that “ibrahim-alsayed.net” was registered on or about December 21, 2016.

g. A search of publicly available Whois domain name registration records revealed that “naimkassem.net” was registered on or about September 1, 2006.

h. A search of publicly available Whois domain name registration records revealed that “alemdad.net” was registered on or about September 6, 2006.

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

40. As described above, Lebanese Hizballah is a designated SDN and Foreign Terrorist Organization. Also as described above, the SUBJECT DOMAIN NAMES are assets of Lebanese Hizballah and its affiliated individuals, entities, organizations, or sources of influence over Lebanese Hizballah and its affiliated entities or organizations within the meaning of 18 U.S.C. § 981(a)(1)(G)(i). As a result, the SUBJECT DOMAIN NAMES are subject to seizure and forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i) as domestic assets: (i) of Lebanese Hizballah -- and its affiliated individuals, entities, and organizations -- a designated foreign terrorist organization, which has engaged in planning and perpetrating federal crimes of terrorism as defined in 18 U.S.C. § 2332b(g)(5) against the United States, citizens or residents of the United States, or their property; or (ii) affording a person a source of influence over Lebanese Hizballah and its affiliated entities and organizations. The same SUBJECT DOMAIN NAMES are subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(G)(i) and 28 U.S.C. § 2461(c).

41. Title 18, United States Code, Section 981(b) authorizes seizure of property subject to civil forfeiture based upon a warrant supported by probable cause.

42. Title 21, United States Code, Section 853(f), applicable here through Title 28, United States Code, Section 2461(c), authorizes the issuance of a criminal seizure warrant. Title 21, United States Code, Section 853(f) provides in relevant part that a seizure warrant for property subject to forfeiture may be sought in the same manner in which a search warrant may be issued. A court shall issue a criminal seizure warrant if it determines that the property to be seized would, in the event of a conviction, be subject to forfeiture and that a restraining order would be inadequate to assure the availability of the property for forfeiture.

43. Neither a restraining order nor an injunction is sufficient to guarantee the availability of the SUBJECT DOMAIN NAMES for forfeiture. By seizing the SUBJECT DOMAIN

NAMES and redirecting it to another domain, the Government will prevent third parties from acquiring the name and using it to commit additional crimes. Furthermore, seizure of the SUBJECT DOMAIN NAMES will prevent third parties from continuing to access the subject domain websites in their present form.

44. Title 28, United States Code, Section 1395(b) provides that venue for civil forfeiture actions is proper in any district where the subject property is found.

45. Since criminal forfeiture is an aspect of the defendant's sentencing, venue for a criminal forfeiture lies wherever venue for a criminal prosecution is proper.

SEIZURE PROCEDURE

46. As detailed in Attachment A, upon execution of the seizure warrant, the registry for the SUBJECT DOMAIN NAMES, Verisign, Inc., located at 12061 Bluemont Way, Reston, Virginia 20190, and the Public Interest Registry, located at 11911 Freedom Drive, Reston, Virginia 20190, shall be directed to restrain and lock the SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with U.S. government law enforcement or the Department of Justice.

47. In addition, upon seizure of the SUBJECT DOMAIN NAMES by U.S. government law enforcement or the Department of Justice, VeriSign and PIR will be directed to associate the SUBJECT DOMAIN NAMES to a new authoritative name server(s) to be designated by a law enforcement agent. The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve indicating that the site has been seized pursuant to a warrant issued by this court.

CONCLUSION

48. For the foregoing reasons, I submit that there is probable cause to believe that the SUBJECT DOMAIN NAMES constitute assets of entities and organizations engaged in planning or perpetrating a federal crime of terrorism against the U.S., its citizens and residents, and their property. The SUBJECT DOMAIN NAMES also afford a source of influence over those entities and organizations. Accordingly, the SUBJECT DOMAIN NAMES are subject to civil forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(G)(i), and criminal forfeiture through those same statutes as incorporated by 28 U.S.C. § 2461(c), and I respectfully request that the Court issue a seizure warrant for SUBJECT DOMAIN NAMES.

49. Because the warrant will be served on Verisign and PIR, which controls the SUBJECT DOMAIN NAMES, and Verisign and PIR, thereafter, at a time convenient to it, will transfer control of the SUBJECT DOMAIN NAMES to the government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

**TINA
CHANG**

Digitally signed by TINA
CHANG
Date: 2023.05.01
10:25:21 -04'00'

Tina Show-Hwa Chang
Special Agent
Bureau of Industry and Security
U.S. Department of Commerce

Attested to by the applicant in accordance with
the requirements of Fed. R. Crim. P. 4.1 by telephone
on May 2, 2023:

Lindsey Vaala

Digitally signed by Lindsey Vaala
Date: 2023.05.02 09:35:54 -04'00'

Hon. Lindsey R. Vaala
United States Magistrate Judge
Alexandria, Virginia

ATTACHMENT A

1) With respect to “moqawama.org,” “almanarnews.org,” “manarnews.org,” “almanar-tv.org,” and “alshahid.org,” (hereinafter the “SUBJECT DOMAIN NAMES”), the Public Interest Registry (PIR), which is the domain registry for the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of the SUBJECT DOMAIN NAMES:

2) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Department of Justice and the Department of Commerce, by updating the authoritative nameservers for the SUBJECT DOMAIN NAMES to:

- (a) ns-1088.awsdns-08.org;
- (b) ns-1900.awsdns-45.co.uk;
- (c) ns-388.awsdns-48.com;
- (d) ns-977.awsdns-58.net; and/or
- (e) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Registrar.

3) Prevent any further modification to, or transfer of, the SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with Department of Justice and the Department of Commerce

4) Take all reasonable measure to propagate the necessary changes through the Domain Name System as quickly as practicable.

5) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

6) The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve. That notice will consist of law enforcement emblems and the following text:

The domain for the SUBJECT DOMAIN NAMES has been seized by the United States Government in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981 and 50 U.S.C. §§ 1701-1705 as part of a law enforcement action by the Bureau of Industry and Security, Office of Export Enforcement.

ATTACHMENT A

1) With respect to “manarnews.net,” “manartv.net,” “almanar-tv.com,” “almanar-tv.net,” “alidaamouch.com,” “ibrahim-alsayed.net,” “naimkassem.net,” and “alemdad.net,” (hereinafter the “SUBJECT DOMAIN NAMES”), VeriSign, Inc., which is the domain registry for the SUBJECT DOMAIN NAMES, shall take the following actions to effectuate the seizure of the SUBJECT DOMAIN NAMES:

2) Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Department of Justice and the Department of Commerce by associating the SUBJECT DOMAIN NAMES to the following authoritative name-servers:

(a) ns-1088.awsdns-08.org;

(b) ns-1900.awsdns-45.co.uk;

(c) ns-388.awsdns-48.com;

(d) ns-977.awsdns-58.net; and/or

(e) Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including e-mail, to the Registrar.

3) Prevent any further modification to, or transfer of, the SUBJECT DOMAIN NAMES pending transfer of all right, title, and interest in the SUBJECT DOMAIN NAMES to the United States upon completion of forfeiture proceedings, to ensure that changes to the SUBJECT DOMAIN NAMES cannot be made absent court order or, if forfeited to the United States, without prior consultation with the Department of Justice and the Department of Commerce

4) Take all reasonable measure to propagate the necessary changes through the Domain Name System as quickly as practicable.

5) Provide reasonable assistance in implementing the Terms of this Order and take no unreasonable action to frustrate the implementation of this Order.

6) The Government will display a notice on the website to which the SUBJECT DOMAIN NAMES will resolve. That notice will consist of law enforcement emblems and the following text:

The domain for the SUBJECT DOMAIN NAMES has been seized by the United States Government in accordance with a seizure warrant issued pursuant to 18 U.S.C. § 981 and 50 U.S.C. §§ 1701-1705 as part of a law enforcement action by the Bureau of Industry and Security, Office of Export Enforcement.